IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
Alexandria Division

UNITED STATES OF AMERICA, Plaintiff, v. ZACKARY ELLIS SANDERS, Defendant.	Case No. 1:20-cr-00143 Honorable T.S. Ellis, III Sentencing: April 1, 2022

REPLY IN SUPPORT OF DEFENDANT'S MOTION FOR RETURN OF PROPERTY AND RESPONSE IN OPPOSITION TO THE GOVERNMENT'S MOTION FOR A PRELIMINARY ORDER OF FORFEITURE

Zackary Ellis Sanders files this reply in support of his motion for return of property (ECF No. 608, hereinafter "Mot.") and responds in opposition to the government's motion for a preliminary order of forfeiture (ECF No. 610, hereinafter "Opp."). Forfeiture in this case must be limited to the contraband material (*e.g.*, illegal images) and the electronic devices that housed it. It cannot encompass non-contraband files and data that reasonably can be identified and segregated at the expense of Mr. Sanders. Non-contraband computer files are distinct property, separate and apart from the devices in which they are contained, and there is no legal basis to subject such property to forfeiture. In the alternative, this Court should continue the forfeiture component of its sentencing to permit the Court to hold an evidentiary hearing to consider the work that would be involved in segregating and returning the non-contraband computer files to Mr. Sanders.

A. The government's motion for a preliminary forfeiture order is untimely.

As an initial matter, the government's motion for a preliminary forfeiture order is untimely. Rule 32.2(b)(2)(B) requires the court to "enter the preliminary order sufficiently in

advance of sentencing to allow the parties to suggest revisions or modifications before the order becomes final as to the defendant under Rule 32.2(b)(4)," unless doing so is impractical. Fed. R. Crim. P. 32.2(b)(2)(B). The government omits this requirement when discussing the procedure for resolving the motion. *See* Opp. at 17. As the government acknowledges, Opp. at 17, a preliminary order "becomes final as to the defendant," at the latest, at sentencing.[1] Fed. R. Crim. 32.2(b)(4)(A).

Here, with no explanation for its timing, the government filed its motion for a preliminary forfeiture order just *three days* before sentencing, and only in response to Mr. Sanders's motion for return of property, leaving Mr. Sanders insufficient time to respond adequately to the government's motion. Fed. R. Crim. P. 32.2(b)(1)(A), (b)(2)(A)-(B). More important, the government has left the Court with insufficient time to consider the novel legal issues and complex factual concerns presented prior to tomorrow's sentencing, much less to meet its obligation under Rule 32.2(b)(2)(B) to enter a preliminary order sufficiently in advance of sentencing to allow for suggested revisions and modifications. *See, e.g., United States v. Shakur*, 691 F.3d 979, 988–89 (8th Cir. 2012) (finding that "wholesale violation" of Rule 32.2(b) mandates—timely determination of the "requisite nexus," "the entry of a preliminary order," and "entry of that order 'sufficiently in advance of sentencing' to allow him to seek revisions"—denies a defendant his due process rights).

Forfeiture is a form of punishment, *Austin v. United States*, 509 U.S. 602, 622 (forfeiture is punishment subject to the Eighth Amendment's Excessive Fines Clause), and therefore implicates due process concerns. The Court should not permit the government to shortcut the

[1] As the government acknowledges, the preliminary order remains preliminary as to third parties until any ancillary proceeding addressing those third-party claims is concluded under Rule 32.2(c). *See* Fed. R. Crim. P. 32.2(b)(4).

process through its late filing. Unless the Court denies the government's motion, it should at least continue sentencing to permit further proceedings on the issue of forfeiture, including a hearing to consider the relative burdens of returning the non-contraband computer files to Mr. Sanders. *See* Fed. R. Crim. P. 32.2(b)(1)(B) (requiring a hearing if either party requests one).

B. Non-contraband electronic files and data are not subject to forfeiture, even if the device in which they are contained is subject to forfeiture.

As to the merits, the crux of the issue is whether, for purposes of criminal forfeiture, the files of a computer are separate items of property distinct from the electronic device in which they are contained. Accepted notions of property, as well as the language of the forfeiture statute, its structure, and purpose, all support the interpretation that such files are property distinct from the devices on which they reside, and that non-contraband files that are not shown by the government to have been used to facilitate the offenses cannot be subject to forfeiture.

The government makes much about many things that are not at issue, presumably in an attempt to color the issue as more complicated and difficult than it actually is. For example, the government repeatedly discusses the nine devices that allegedly contain contraband. *See* ECF No. 610 at 1, 7, 8, 10, 13 & 18; ECF No. 610-1 at 2-4; ECF No. 610-2 at 2. Indeed, the government's entire argument about undue burden is premised on the alleged involvement of *all* files on *all* nine devices in Mr. Sanders's proposed review. *See, e.g.*, Ex. 2 at 2-4 (discussing, among other things, "3 [terabytes] of digital storage to review"). But, as the government knows from its discussions with Mr. Sanders's counsel, Mr. Sanders is asking only for the return of certain types of non-contraband files from three of those devices, an iPhone, an iPad, and a laptop computer. The government also spends an inordinate amount of space in its response and the accompanying declaration laying out the number of alleged contraband images and what those photos depict, *see* Ex. 2 at 2-4, but Mr. Sanders is not requesting the return of any

contraband images and is not contesting forfeiture of the devices themselves (as opposed to the non-contraband contents).[2] *See* Mot. at 3; *see also United States v. Martin*, 662 F.3d 301, 309 (4th Cir.2011) ("[T]he substantive purpose of criminal forfeiture is ... to deprive criminals of the fruits of their illegal acts and deter future crimes."), *cert. denied*, 566 U.S. 955 (2012). Thus, the number of alleged contraband images or their descriptions is irrelevant to the issue at hand.

The government also stresses that forfeiture is mandatory. While it is true that property meeting the statutory criteria must be forfeited, the government bears the burden of showing that those statutory criteria are met. Fed. R. Crim. P. 32.2(b)(1)(A) ("If the government seeks forfeiture of specific property, the court must determine whether the government has established the requisite nexus between the property and the offense."); *see also United States v. Bailey*, 926 F. Supp. 2d 739, 761 (W.D.N.C. 2013) ("Before a preliminary order of forfeiture is entered, a judicial determination must be made as to whether the 'requisite nexus' exists between the property to be seized and the offenses of conviction . . . [T]he Government bears the burden of proving nexus by a preponderance of the evidence.") (citing *United States v. Cherry*, 330 F.3d 658, 669–70 (4th Cir.2003)). Mandatory forfeiture does not absolve the government of its burden of proof. If the government does not show that the statutory criteria are met for a particular piece of property, forfeiture of that piece of property is, of course, not mandatory. Indeed, such forfeiture is precluded. Fed. R. Crim. P. 32.2(b)(1)(A).

Putting aside these distractions, the government argues that non-contraband files are subject to forfeiture under two statutory provisions. First, it argues that, under 18 U.S.C. §

[2] Indeed, the government's detailed discussion of the number of alleged contraband images and what they allegedly depict only undermines the government's argument by showing that they have already identified the contraband images on each device.

2253(a)(1), such files are subject to forfeiture because the electronic devices in which they are contained constitute "other matter[s] which contain any such visual depictions." Mr. Sanders, however, does not dispute that the electronic devices themselves, separate and apart from any files on them, are subject to forfeiture. The statute does not provide that such "matters" *and all of their contents* are subject to forfeiture. Indeed, the statute separately provides for the forfeiture of contraband images on such devices, first requiring forfeiture of "any visual depiction" and then "other matter[s] that contain any such visual depictions." 18 U.S.C. § 2253(a)(1). As applied to electronic devices containing contraband images, this shows (a) a computer and its files are separately considered under the statute and (b) only files that are contraband are subject to forfeiture.

The government's attempt to analogize the thousands of computer files to a book, magazine, periodical, film, or videotape, ECF No. 610 at 14-15, is inapt. One cannot equate the thousands of various unrelated files on a phone or computer with a discrete item like a book, where all such pages were published together. Indeed, a book, magazine, or periodical in electronic format is typically a single file on a computer. A film or videotape is equivalent to a video file on a computer. Contrary to the government's analogy, the individual pages of a magazine are not stored in individual files. Rather, the many files on a computer or phone are more analogous to the thousands of books in a library. Particular books (*e.g.,* files) within a particular collection (*e.g.,* a computer) containing contraband images may be subject to forfeiture, but not the many other books within the collection that have no relation to the contraband and are not contraband themselves. *See, e.g., Computer File*, Wikipedia (Mar. 13, 2022), available from https://en.wikipedia.org/wiki/Computer_file (last accessed Mar. 31, 2022) ("A computer file is a computer resource for recording data in a computer storage device,

primarily identified by its file name. Just as words can be written to paper, so can data be written to a computer file. Files can be shared with and transferred between computers and mobile devices via removable media, networks, or the Internet.").

Second, the government argues that the non-contraband files are subject to forfeiture under subsection 2253(a)(3), which provides for forfeiture of "any property, real or personal, used or intended to be used to commit or to promote the commission of such offense or any property traceable to such property." 18 U.S.C. § 2253(a)(3). Mr. Sanders, of course, is not asking for the return of any property, whether devices or files, that were allegedly used or intended to be used to commit the offenses in this case. Accordingly, if one accepts the indisputable premise that computer files are property, separate and distinct from the device on which they reside, then section 2253(a)(3) is inapplicable on its face. Even if the Court were to conclude that section 2253(a)(3) is ambiguous as to non-contraband computer files, the rule of lenity applicable to criminal law would require the Court to construe it in Mr. Sanders's favor. *See United States v. R.L.C.*, 503 U.S. 291, 293 (1992) ("No ambiguity about the statute's intended scope survives the foregoing analysis, but if any did, the construction yielding the shorter sentence would be chosen under the rule of lenity."); *Chapman v. United States*, 500 U.S. 453, 463 (1991) (A statute must be ambiguous for the rule of lenity to apply.); *Bifulco v. United States*, 447 U.S. 381, 387 (1980) (The rule of lenity "means that the Court will not interpret a federal criminal statute so as to increase the penalty that it places on an individual when such an interpretation can be based on no more than a guess as to what Congress intended."); *Larue v. Adams*, No. 1:04-0396, 2006 WL 1674487, at *15 (S.D.W. Va. June 12, 2006) ("The rule of lenity . . . requires that ambiguities in criminal or punitive statutes must be resolved in favor of the [defendant].").

The government relies heavily on *United States v. Noyes*, 557 Fed. Appx. 125 (3d Cir. 2014), an unreported decision in which the court ruled against a pro se motion on procedural grounds. ECF No. 610 at 8-9, 11. But *Noyes* did not address the precise issue presented here—whether the files on a computer constitute property separate and apart from the computer in which they are contained. The court in *Noyes* stressed that section 2253(a) included "'*any property* … used or intended to be used to commit or to promote the commission of such offense,'" and that there is "nothing in the statute which indicates that only a portion of the 'property' can be forfeited. *Noyes,* 557 Fed. Appx. at 127 (quoting 18 U.S.C. § 2253(a)(3) (emphasis in original). The question *Noyes* skipped over is whether the computer files are indeed "a portion," i.e., part of, the device or are they property in and of themselves. As discussed above, they are clearly the latter. And if they are the latter, there is no basis for their forfeiture.[3]

From this, several principles should be undisputed. First, the Court may order forfeiture of an electronic device itself under either section 2253(a)(1) (devices containing contraband images) or 2253(a)(3) (devices "used" for committing the offenses) where the government satisfies its burden of proof. Mr. Sanders has never contended otherwise. Second, as a corollary, a device used to perpetrate the offense may be forfeited under section 2253(a)(3) even if it contains no contraband images (or any files whatsoever), *e.g.*, if the device had been "wiped" of all data prior to or after its seizure. Under section 2253(a)(3), it is the device that was allegedly used, not the non-contraband files. In other words, whether a device is forfeitable under section

[3] The only case the government cites on this issue from this District is *United States v. Hoffman*, No. 2:12cr184, 2018 WL 5973763 (E.D. Va.). In *Hoffman*, an espionage case involving a consent forfeiture order, the court relied exclusively on the reasoning of *Noyes*, noting that there was also no language in the applicable forfeiture statute "indicating that only a portion of the forfeited property can be forfeited." *Hoffman*, 2018 WL 5973763, at *3.

2253(a)(3) has nothing to do with the files it contains.[4] Thus, section 2253(a)(3) is satisfied if the relevant devices are forfeited, with or without any files on the devices.

Third, computer files indisputably are property in and of themselves—regardless of their storage on a cell phone or other computer device. *See, e.g., Riley v. California,* 573 U.S. 373, 393–94 (2014) ("The term 'cell phone' is . . . misleading shorthand; many of these devices are in fact minicomputers that also happen to have the capacity to be used as a telephone. They could just as easily be called cameras, video players, rolodexes, calendars, tape recorders, libraries, diaries, albums, televisions, maps, or newspapers. One of the most notable distinguishing features of modern cell phones is their immense storage capacity. Before cell phones, a search of a person was limited by physical realities and tended as a general matter to constitute only a narrow intrusion on privacy. . . . Most people cannot lug around every piece of mail they have received for the past several months, every picture they have taken, or every book or article they have read—nor would they have any reason to attempt to do so. And if they did, they would have to drag behind them a trunk . . . , rather than a container the size of [a] cigarette package.").

Fourth, of course, non-contraband files that are *not* contained within a forfeitable device cannot be subject to forfeiture. This is true even if such files were previously on a device subject to forfeiture. For example, if a defendant transfers family photos from a forfeitable device to another untainted device *prior to seizure*, the non-contraband files on the new device unquestionably would not be subject to forfeiture. It stands to reason then, that if those same files are transferred or copied from a forfeitable device to another device *after seizure*, they are also not subject to forfeiture.

[4] Of course, files on a particular device, such as contraband images, messages, etc., may help prove the required nexus between the device and the offenses, but they are not necessary to do so and are not the legal basis for forfeiture under section 2253(a)(3).

In sum, there is no basis to order forfeiture of non-contraband computer files or data under section 2253(a)(1) because they are neither a visual depiction described in the relevant statutes (i.e., contraband images), nor are they a "portion" of a "matter which contains any such visual depiction." They are separate and distinct property from the container in which they are found. The devices are forfeitable whether or not they contain such non-contraband files.

In addition, there is no basis to order forfeiture of non-contraband computer files under section 2253(a)(3) because it is only the device that was "used or intended to be used to commit" the relevant offenses. The non-contraband files on the device are separate and distinct property that are not used or intended to be used in such a manner. If the non-contraband files are transferred from the computer, the computer is still subject to forfeiture. Simultaneously, if such files are transferred from the computer, there is no basis to seek their forfeiture.

C. Returning the non-contraband computer files to Mr. Sanders would not be burdensome.

What is left is only whether copying or transferring the limited universe of non-contraband files and data from the three devices, and double-checking that those files do not contain contraband images, would be unduly burdensome, as the government claims. Arguably, the burden of returning property that cannot legally be subject to forfeiture should not be relevant. If there were two files on a computer—one was contraband and one was not—there would be no question that the non-contraband file should be returned. But in any event, what Mr. Sanders is asking would not be unduly burdensome, especially in view of the important nature of the files and the fact that they are not subject to forfeiture.

As Mr. Sanders's counsel has informed the government, Mr. Sanders will bear any costs of the work needed to find, segregate, and copy or transfer files that are not subject to forfeiture. That process would involve searching for certain file types (*e.g.*, .doc, .pdf, etc.), which can be

done through an automated process by Mr. Sanders's forensic expert. For image and video files, and to double-check the files segregated for copying for return to Mr. Sanders, the government can use the same automated software it uses to locate contraband images on a device, *e.g.*, the Griffeye tool mentioned in Mr. Sanders's motion. *See* Mot. at 2.

In response, the government raises the specter that it would need to review tens of thousands of files before any material could be released and that Griffeye, its automated software tool, could not be used because it can only detect images previously identified and categorized as child pornography. See Opp. Ex. 1, Kochy Decl. at 3-4. This is a red herring. First, the government greatly exaggerates the number of files that would be candidates for segregation. It cites 3 TB of digital data and speculates that such an amount of data could result in 750,000 pictures and 78 business days of review. *Id.* at 3 (stating that it "could" result in 750,000 pictures and that the 78 days assumes that "the defense export[s] all of these files"). This unrealistic scenario presumably covers all nine devices, which, as reviewed above, greatly overstates the universe of all data involved. Second, even within the three devices at issue, Mr. Sanders's expert would not be exporting all files.[5] As explained to the government and reviewed in Mr. Sanders's motion, Mr. Sanders seeks the return of only certain, discrete types of personal files.

[5] Indeed, a significant portion of the 3 TB of stored data cited by the government is presumably made up of "system files," as opposed to user-created files. Substantial numbers of such system files are found on every electronic computerized device, including smart phones, tablets, and computers, and are necessary for the device and its software to operate. They are easily segregable and normally not even readable by humans, and certainly would not be sought by Mr. Sanders. *See, e.g., System File*, Wikipedia (Mar. 9, 2022), available from https://en.wikipedia.org/wiki/System_file (last accessed Mar. 31, 2022) ("A system file in computers is a critical computer file without which a computer system may not operate correctly. These files may come as part of the operating system, a third-party device driver or other sources.").

The government's assertion that it would need to manually review every file identified by Mr. Sanders's expert before they could be turned over is simply not credible. For prosecution purposes, the government certainly does not manually review every single file on a device that is seized from a defendant that has potentially millions of files to determine if each file is contraband; it uses specialized software for that. As the government explains, the Griffeye software is able to identify potential child pornography images using a database of previously identified and categorized images. *Id.* at 5. The government attempts to portray Griffeye as inadequate to review computer files before they are returned to defendants, but that is exactly what the government does when it returns a device on which no child pornography is found. If no child pornography is found on a device and there is no evidence the device was used to commit the alleged offenses, there is no legal basis for the government to retain it, much less subject it to forfeiture. It must return it to the defendant.

If the government's concern voiced here was legitimate, the government would *never* release *any* electronic device to any defendant without manual reviewing every file on the device, even where no contraband images had been found during the investigation. Under the government's reasoning, even if no contraband images were found with automated software during the investigation, the device could still potentially contain contraband images, requiring a human review of every file on the device. The government never does that if no contraband is found on a device. It never does that because it is confident that its automated software works; in fact, the lead agent in this case, FBI Special Agent Ford, demonstrated to the defense how he had already used Griffeye to sort all video and image files on the devices into three different categories: (1) non-child exploitation material; (2) child exploitation material; and (3) "possible" child-exploitation material that required further review. Moreover, it is the government's burden

to prove that property is subject to forfeiture. That includes discrete property in the form of computer files.[6] If it cannot prove that the file is contraband, it should be returned.

CONCLUSION

Because Mr. Sanders retains a property interest in the non-contraband data that is unconnected to criminal activity, this Court should enter an order directing the government to return copies of Mr. Sanders's non-contraband, electronically stored information employing Mr. Sanders's cost and labor shifting proposals for segregating and recovering the non-contraband data on his electronic devices. The Court should also delay entry of a preliminary order of forfeiture until such time as Mr. Sanders's right to the return of his property is decided.

Respectfully submitted,

/s/
Jonathan Jeffress (#42884)
Jade Chong-Smith (admitted *pro hac vice*)
KaiserDillon PLLC
1099 Fourteenth St., N.W.; 8th Floor—West
Washington, D.C. 20005
Telephone: (202) 683-6150
Facsimile: (202) 280-1034
Email: jjeffress@kaiserdillon.com
Email: jchong-smith@kaiserdillon.com

/s/
Nina J. Ginsberg (#19472)
DiMuroGinsberg, P.C.
1101 King Street, Suite 610
Alexandria, VA 22314
Telephone: (703) 684-4333
Facsimile: (703) 548-3181
Email: nginsberg@dimuro.com

[6] The same is true for text messages, chats, emails, and other documents raised by the government. *See id.* at 5. If no such contraband files have been found on a device during the investigation, the device can be returned. The government does not seek forfeiture of a device because it cannot be sure it does not contain contraband files. The same holds true here for the devices where the contraband files have already been identified and are segregable.

/s/
H. Louis Sirkin (admitted *pro hac vice*)
Santen & Hughes
600 Vine Street, Suite 2700
Cincinnati, OH 45202
Telephone: (513) 721-4450
Facsimile: (513) 721-0109
Email: hls@santenhughes.com

Counsel for Defendant Zackary Ellis Sanders

CERTIFICATE OF SERVICE

I hereby certify that on this 31st day of March 2022, the foregoing was served electronically on the counsel of record through the US District Court for the Eastern District of Virginia Electronic Document Filing System (ECF) and the document is available on the ECF system.

/s/ Jonathan Jeffress
Jonathan Jeffress